IMPLEMENTATION OF THE SMART-CONTRACT CONSTRUCTION IN THE LEGAL SYSTEM OF RUSSIA

Rusakova Ekaterina[1], Frolova Eugenia[2], Gorbacheva Anna[3], Ekaterina Kupchina[4]*

[1]Associate professor (Ms.) RUDN University, RUSSIA, rusakova-ep@rudn.ru
[2] Professor, Dr.in Law (Ms.) RUDN University, RUSSIA, frolevgevg@mail.ru
[3]Ms., RUDN University, RUSSIA, anna.gorbachyowa@gmail.com
[4]Associate professor, (Ms.) RUDN University, RUSSIA, belousova-ev@rudn.ru
*Corresponding Author

Abstract

The fourth industrial revolution in the world, or the digital revolution, has a significant impact on the legal systems of all countries of the world, including Russia. The settlement of legal issues concerning the digital transformation of society has become a vital factor in the progressive development of national and cross-border trade, the services sector and the movement of capital.

The aims of this study are, firstly, justification of the feasibility of development and implementation of smart contracts in the legal field, secondly, determination of the legal nature of this construction, thirdly, revealing of legal regulation problems that can appear between parties that decided to regulate their relations by smart contract, fourthly, development of possible solutions to the identified problems.

The article attempts to show smart contract value and the legal nature of the smart contract. Today blockchain, particularly smart contracts can be the solution to many existing financial problems that do not entirely meet the needs of the digital age. The use of paper documents leads to significant time delays and inefficient use of resources and creates the risk of errors and fraud.

The ability to qualify a smart contract as a civil contract depends on what exactly is meant by a smart contract in each particular case, taking into account all ambiguities that exist in the relation of the use of this term.

The authors underline that depending on whether all the stages of the transaction or only their part, are specified in a smart contract, it is possible to select a) a fully automated contract (without paper version), b) partially automated with a copy on paper and c) partially automated, mostly on paper (for example, calculations are governed by a smart contract, the rest of the conditions are defined in a regular contract).

The critical problem of the widespread use of smart contracts is that the parties have to rely on a reliable technical expert to fix their agreement in code, or to confirm that the code written by a third party is correct. The parties will also be interested in ensuring that the code will be executed as they envisage. A possible way to provide such guarantees may be a written contract entered into by the parties with the developer of a smart contract.

The paper insists that in regard of making large transactions, insurance with the warranty agreement with the developer could be an effective tool providing additional protection for the interests of the parties since in the process of the code revising it is likely that parties will not notice the mistakes made by the programmer. Besides, the contracting parties will feel at ease from the fact that the insurance company most likely conducted its own code audit before it agreed to insure a smart contract. The article may be interesting for young lawyers as well as practising lawyers and law students.

Keywords: technology, blockchain, smart contract, cybersecurity, cryptocurrency, risk management.

1 INTRODUCTION

The creation of a system of public blockchains has opened up the possibility for the emergence of a new technology - "smart contracts" that can radically change the perception of contractual relations in the near future. Some participants of the stream of commerce now conclude smart contracts, and the prospect of transition of a considerable part of the contractual relationship to the smart category is not without reason. However, the lack of a legal framework of this construction can cause problems in the regulation of relations between the parties. In this regard, when deciding to enter into a smart contract, the parties should be aware of all possible risks that may arise as a result of non-traditional business relations, as well as be able to use legal tools provided by law in order to prevent the adverse effects of these risks [1].

2 RESEARCH GOALS

The aims of this study are, firstly, the justification of the feasibility of development and implementation of smart contracts in the legal field: secondly, determination of the legal nature of this construction: thirdly, revealing of legal regulation problems that can appear between parties that decided to regulate their relations by a smart contract: fourthly, development of possible solutions to the identified problems.

3 ANALYSIS OF SMART CONTRACT CONSTRUCTION

3.1 Smart contract Value

"Smart contract" is a term used to describe a computer code that automatically fulfils all or part of the agreement between the parties and is stored on a blockchain-based platform. The code itself is replicated on several nodes of the blockchain and, therefore, acquires the properties of security, consistency and immutability, which the blockchain offers.

The “smart” contract independently determines whether everything has been fulfilled, and makes a decision: complete the transaction and issue the required (money, shares, real estate), impose a fine or penalty on participants, close access to assets.

Smart contracts can be the solution to many problems of existing financial instruments that do not entirely meet the needs of the digital age. The use of paper documents leads to significant time delays and inefficient use of resources; creates the risk of errors and fraud. Despite that fact, financial intermediaries minimise such risks and ensure the interaction of many financial market participants; they create additional overhead costs and complicate legal regulation, increasing the costs of requirements compliance [2].

Thus, the main advantages of "smart" contracts are, firstly, the reduction of the chain of intermediaries in a transaction, secondly, self-fulfilment, thirdly, the confidentiality of participants in the transaction and, fourthly, the reduction of the risk of being deceived.

3.2 Legal Nature of a Smart Contract

Among the number of issues arising from the use of blockchain technologies in the legal sphere, the following can be highlighted: Whether a smart contract can be regarded as a legally significant agreement between the parties? The ability to qualify a smart contract as a civil contract depends on what exactly is meant by a smart contract in each particular case, taking into account all the ambiguities that exist in the relation of the use of this term.

According to Art. 420 of the Civil Code of the Russian Federation, the contract is an agreement between two or several persons in regard to establishment, amendment or termination of civil rights and obligations. If the content of the program code is to carry out transactions that constitute an automated equivalent of the actions of the parties that may be subject to a civil law contract, then such a smart contract may well be considered as a legally significant agreement of the parties.

The mere fact that the terms of the contract are presented in the form of program code, does not in itself have a legal meaning since the contract law permits various ways of formalising the agreements of the parties. Russian companies can conclude a legally significant agreement in any language, even in Latin. In this regard, the program code is not much different from another language, since it is understandable for persons with special knowledge of the corresponding programming language. The main thing is that they should allow the possibility of establishing the fact of reaching an agreement between parties under specific conditions.

Under the smart contract, fulfilment of the obligations is an entirely automated process. In this regard, some questions about the potential applicability of provisions concerning obligations to such contracts, procedure for their performance, responsibility for their non-performance or improper performance, and other general provisions arise.

In conditions when a party cannot influence the course of execution, and execution operations are sufficiently programmed, it is difficult to apply rules implying that the party has some will autonomy and, accordingly, the ability to violate the contract or execute it differently. In fact, the will of the parties to conclude and execute a contract is an integrated whole in such smart contracts. Modification and termination of smart contracts by traditional means provided by law is also impossible: such actions must be made in the form of program code, and the necessary level of parties' consensus is to be obtained.

However, the recognition of a smart contract as a contract is not an absolute fiction. Such recognition implies the responsibility for the results of its operation on the parties and therefore does not require the creation of fundamentally new legal structures, for example, for tax purposes. In this regard, the mechanical equating of smart contracts to automata or technical means of copyright protection is counterproductive.

3.3 Kinds of Forms

Depending on whether all the stages of the transaction, or only their part, are specified in a smart contract, it is possible to select a fully automated contract (without hard copy), partially automated with a copy on paper and partially automated, mostly on paper (for example, calculations are governed by a smart contract, the rest of the conditions are defined in a regular contract) [3].

3.4 Smart Contract Development

The critical problem of the widespread use of smart contracts is that the parties have to rely on a reliable technical expert to fix their agreement in a code, or to confirm that the code written by a third party is correct. A person who does not know programming languages is objectively unable to understand even the most straightforward smart contract. In this regard, contracting parties should conclude an additional code decryption agreement [4].

It is worth noting that text templates can be created for many of the essential functions of smart contracts to clarify what parameters need to be entered and how these parameters should be performed in an electronic environment, so to say "instructions for use."

As an example, it is useful to consider the simple function of a smart contract, according to which, in the event of a delay in the fulfilment of an obligation, the amount payable is automatically deducted from the counterparty's electronic wallet. The text template may contain information on how the amount of the expected payment should be indicated in the code of the smart contract, the date of performance and liability for late payment.

However, the parties may wish to confirm the fact that the base code performs the functions specified in the text and that it is not necessary to set additional conditions or parameters. This is especially true if the text template excludes any liability arising from the correctness of the underlying code. To conduct such verification, the parties will still need to contact a trusted third party with some knowledge of programming.

The parties will obviously also be interested in ensuring that the code will be executed precisely as they envisage. A possible way to provide such guarantees may be a written contract concluded by the parties with the developer of a smart contract.

For the same purpose, the parties could in the future contact insurance companies where the risk that the smart contract code does not fulfil the functions specified in the text of the agreement will be insured. In regard of making large transactions, insurance with the warranty mentioned above agreement with the developer could be an effective tool providing additional protection for the interests of the parties, since in the process of the code revising it is likely that parties will not notice the mistakes made by the programmer. Besides, the contracting parties will feel at ease from the fact that the insurance company most likely conducted its own code audit before it agreed to insure a smart contract.

3.5 Getting Resources "Out of the Chain"

In certain situations, the use of a smart contract as a regulator of legal relations between the parties may entail the need to obtain information from sources that are not in the chain of blocks, so-called, resources outside the network. For example, a crop insurance smart contract is programmed to transfer the insurance value to a party if the temperature falls below 0 degrees Celsius during the summer. In this situation, a smart contract will have to obtain temperature data from an agreed source to regulate the fulfilment of the obligation.

The implementation of this condition is hampered by two points. First, smart contracts cannot extract data from off-line resources; that is, such information must be provided to the contract by a third source. Secondly, if the data is in a constant stream, different nodes can receive different information, since the code is replicated through several nodes over the network, as a result of which the information can reach the "smart" contract in a distorted form.

In the above example, Node-1 can receive information that the temperature is 1°C, and Node-2, in turn, can receive information that the temperature is actually 0°C. Given that each transaction to be verified requires a consensus regarding information transfer nodes, such deviations may lead to a condition in the relation of insured value payment will be considered "not satisfied".

Contracting parties will be able to solve this puzzle, by using the so-called "oracles". Oracle is a set of programs inside and outside the blockchain for transferring information from the outside world into the blockchain in the automatic mode in a format understandable to it (blockchain). Oracles are third parties trusted by the parties. They provide the necessary information from the outside world that affects the execution of a software algorithm to monitor the implementation of conditions by a smart contract. They can be any data - temperature, price change, payment status, and others. Oracles are the only way for smart contracts to interact with the external environment outside the blockchain [5].

In our example, the oracle will monitor the daily temperature, detect the time when frost occurred, and then transmit this information to the smart contract.

Although oracles can be considered as a solution to the problem of accessing resources outside the network, this process requires the involvement of a third party, an oracle application provider, with whom a contract for the subsequent implementation of a smart contract must be concluded. This fact definitely blurs the benefits of a smart contract, such as efficiency and reduction of intermediaries in a transaction [6].

Such a process is also fraught with potential "failures". For technical reasons, information may be delayed or unavailable. For example, if the site of the official source of information broke. Also, the oracle itself may have systemic flaws. In certain situations, these flaws can cause the inability of an oracle to provide the necessary information or transmit erroneous data or an oracle to leave the business chain. Thus, such situations should be considered by the parties in a written agreement.

3.6 Automated Nature of Smart Contracts

One of the critical features of smart contracts is their ability to automatically and continuously execute transactions without the need for human intervention. However, such automation, coupled with the fact that smart contracts cannot be easily changed or terminated (unless, of course, the parties included such opportunities during the creation of a smart contract), is one of the biggest challenges for a wide distribution of smart contracts.

For example, when a traditional contract has been concluded, the party may forgive the violation of the counterparty and not apply the available sanctions. If a valuable customer is late with a one-month payment, the seller can decide in real time that the preservation of long-term commercial relations is more important than the realisation of the right to unilaterally refuse to fulfill obligations or to recover a penalty for late payment. However, if this relationship were based on a smart contract, the option of derogating ad hoc from contractual clauses regarding the imposition of sanctions would be objectively impossible.

Delay of payment will automatically lead to automatic debiting of the amount payable from the client’s account or suspension of the client’s access to the software or a device connected to the Internet if a smart contract has been programmed to this object. Thus, the automatic execution carried out by smart contracts is inherently a rigid regulation, which does not take into account all sorts of human and other factors that in one degree or another affect the performance of contractual obligations [6].

Similarly, in a relationship mediated by a traditional contract, a party in certain situations may agree to accept a partial performance, which will be credited as full. Such behaviour of the party may be associated, firstly, with interest in maintaining long-term business relationships with the client, and, secondly, with the decision of the party in its preference to get a partial performance than not to get performance at all. Here, again, the excessive formality inherent in the smart contract code may not reflect the realities of interaction between the parties in the commercial exchange.

3.7 Payment Guarantee

One of the advantages often attributed to "smart" contracts is that they can automate payment without the need for notifications or other costs, and also without the need to go to court to obtain a writ of execution for debt collection. Such conditions, indeed, are a relatively reliable way of safeguarding the interests of the parties; however, in complex commercial relations automatic collection may not always be implemented.

The reality is that the funds of an organisation are constantly in circulation, and it is unlikely to keep the total amount required to repay obligations under a long-term contract in its e-wallet. In the same way, a person receiving a loan is unlikely to keep the full amount of the loan in a wallet linked to a smart contract.

Thus, if a party fails to finance its e-wallet promptly, the smart contract that governs this legal relationship and which, accordingly, in the event of non-payment on the specified date should automatically deduct funds, may face the impossibility of recovery due to the lack of these funds in the wallet. The introduction of an additional function in a "smart" contract that establishes, for example, the possibility of debiting funds from other e-wallets or the possibility of filling a purse with funds from other sources does not solve the problem if these wallets or sources of funds also do not have the required payment amounts [7].

The parties may try to solve this problem by including in the supplementary agreement, concluded in the traditional form, the requirement that the wallet associated with the smart contract always have a minimum amount. However, such a condition would not make the payment on a smart contract fully automatic. It only could strengthen the legal position of the party as a legal basis for the recovery of the amount of the debt. Thus, even though smart contracts do help simplify payment, they cannot eliminate the need to resolve debt collection disputes.

4 CONCLUSIONS

Based on the above, several practical conclusions can be drawn:

A smart contract can be regarded as a legally significant agreement between the parties.

At present, parties wishing to regulate their relations by a smart contract should choose a hybrid contractual relationship model combining a text and a code, that is, a partially automated contract. With this approach, the parties can see and understand the agreed terms, or include other conditions that cannot be enforced by a smart contract, and will also have an objectified document to which they can refer in court in the event of a dispute.

The textual part of the so-called "hybrid" contract should contain the clearly indicated code of the smart contract with which this written contract is associated. Besides, it is necessary to specify the variables to be transferred to the smart contract, particularly, how they are defined, and the transaction events that will trigger the execution of the code.

Parties will need to involve third-party technical experts to verify the code. They can also enter into a warranty agreement with a programmer who has developed or verified a smart contract code.

If the parties decide to use oracles to obtain data from the outside world, they should settle in advance the issue of resolving the situation, when the oracle cannot provide the necessary data, transmit erroneous data or just exit the process.

Parties should consider the prospective risk allocation situation in the event of a coding error or hacker attack.

The text agreement accompanying the code should include provisions concerning the order of priority of the text and the code in the event of a conflict, as well as the applicable law and the place of dispute resolution if the transaction is of a cross-border nature.

The text agreement must include the assurance by each party that they have verified the code of the smart contract and are convinced that it reflects the conditions contained in the text agreement. Such an assurance is unlikely to force the parties actually to study the code in detail; however, it will be able to help the counterparty defend itself against a possible statement of the other party that the code was not verified.

Parties should insure the risk of errors in the code.

5 ACKNOWLEDGEMENT

The research is implemented within the framework of the RUDN university participation in the Russia-wide 5-100 project.

REFERENCE LIST

Dudin, M.N., Frolova, E.E., Lubenets, N.A, Sekerin, V. D., Bank, S.V., Gorokhova, A.E. (2016). Methodology of analysis and assessment of risks of the operation and development of industrial enterprises. Quality - access to success. 17 (153). https://elibrary.ru/item.asp?id=26553567

Smart Contracts in Financial Services: Getting from Hype to Reality. (2016) Capgemini Consulting. p. 2. https://www.capgemini-consulting.com/blockchain-smart-contracts

Mikhailova, A. (2018) Smart contracts: how they work and why they are needed. https://pravo.ru/story/205151/

Levi Stuart, D., Lipton Alex, B. (2018). An Introduction to Smart Contracts and Their Potential and Inherent Limitations. Skadden, Arps, Slate, Meagher & Flom LLP, on Saturday. https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/.

Oracle in ethereum, (2017). URL: https://bitcryptonews.ru/blogs/blokchejn/orakulyi-v-efiriume

Dudin, M.N., Zasko, V.N., Frolova, E.E., Pavlova, N.G., Rusakova, E.P. (2018). Mitigation of cyber risks in the field of electronic payments: organizational and legal measures. Journal of advanced research in law and economics. 9 (1). https://elibrary.ru/item.asp?id=35790637

Frolova, E.E., Polyakova, T.A., Dudin, M.N., Rusakova, E.P., Kucherenko, P.A. (2018). Information security of Russia in the digital economy: the economic and legal aspects Journal of Advanced Research in Law and Economics. 9. (1). https://elibrary.ru/item.asp?id=35790834.